The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
212cafe -- 212cafeboard	SQL injection vulnerability in view.php in 212cafe Board 0.07 allows remote attackers to execute arbitrary SQL commands via the qID parameter.	2008-10-23	7.5	CVE-2008-4713 XF BID MILW0RM
arabcms -- arabcms	Directory traversal vulnerability in rss.php in ArabCMS 2.0 beta 1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the rss parameter.	2008-10-22	7.5	CVE-2008-4667 BID MILW0RM FRSIRT
arzdev -- gemini_portal	Multiple PHP remote file inclusion vulnerabilities in The Gemini Portal 4.7 allow remote attackers to execute arbitrary PHP code via a URL in the lang parameter to (1) page/forums/bottom.php and (2) page/forums/category.php.	2008-10-23	9.3	CVE-2008-4720 BID MILW0RM
astrospaces -- astrospaces	SQL injection vulnerability in profile.php in AstroSPACES 1.1.1 allows remote attackers to execute arbitrary SQL commands via the id parameter in a view action.	2008-10-21	7.5	CVE-2008-4642 BID MILW0RM SECUNIA
atomic_photo_album -- atomic_photo_album	Atomic Photo Album 1.1.0 pre4 does not properly handle the apa_cookie_login and apa_cookie_password cookies, which probably allows remote attackers to bypass authentication and gain administrative access via modified cookies.	2008-10-23	7.5	CVE-2008-4714 BID MILW0RM
aves -- rpg_board	SQL injection vulnerability in index.php in RPG.Board 0.8 Beta2 and earlier allows remote attackers to execute arbitrary SQL commands via the showtopic parameter.	2008-10-24	7.5	CVE-2008-4736 XF BID MILW0RM BUGTRAQ

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
bosdev -- bosnews	SQL injection vulnerability in news.php in BosDev BosNews 4.0 allows remote attackers to execute arbitrary SQL commands via the article parameter.	2008-10-23	7.5	CVE-2008-4703 XF BID MILW0RM
cisco -- ios microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_286 microsoft -- windows_386 microsoft -- windows_95 microsoft -- windows_98 microsoft -- windows_98se microsoft -- windows_9x microsoft -- windows_ce microsoft -- windows_me microsoft -- windows_mobile microsoft -- windows_nt microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.	2008-10-20	7.1	CVE-2008-4609 MISC MISC CISCO MISC MLIST MISC
cisco -- adaptive_security_appliance_5500_series cisco -- pix_security_appliance	Unspecified vulnerability in Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.2(4)9 and 7.2(4)10 allows remote attackers to cause a denial of service (device reload) via a crafted IPv6 packet.	2008-10-23	7.8	CVE-2008-3816 CISCO
cisco -- adaptive_security_appliance_5500_series cisco -- pix_security_appliance	Memory leak in Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 8.0 before 8.0(4) and 8.1 before 8.1(2) allows remote attackers to cause a denial of service (memory consumption) via an unspecified sequence of packets, related to the "initialization code for the hardware crypto accelerator."	2008-10-23	7.8	CVE-2008-3817 CISCO
coastal -- coast	PHP remote file inclusion vulnerability in header.php in Concord Asset, Software, and Ticket system (CoAST) 0.95 allows remote attackers to execute arbitrary PHP code via a URL in the sections_file parameter.	2008-10-24	9.3	CVE-2008-4735 BID MILW0RM SECUNIA
dart_communications -- powertcp_ftp_for_activex	Buffer overflow in the ActiveX control (DartFtp.dll) in Dart Communications PowerTCP FTP for ActiveX 2.0.2 0 allows remote attackers to execute arbitrary code via a long SecretKey property.	2008-10-21	9.3	CVE-2008-4652 XF BID MILW0RM
datingpro -- matchmaking	SQL injection vulnerability in PG Matchmaking allows remote attackers to execute arbitrary SQL commands via the id parameter to (1) news_read.php and (2) gifts_show.php.	2008-10-22	7.5	CVE-2008-4665 XF BID MILW0RM FRSIRT
elxis -- elxis_cms	Session fixation vulnerability in Elxis CMS 2008.1 revision 2204 allows remote attackers to hijack web sessions by setting the PHPSESSID parameter.	2008-10-21	7.5	CVE-2008-4649 XF BID MISC

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
ftrsoft -- fast_click_sql_lite	PHP remote file inclusion vulnerability in init.php in Fast Click SQL Lite 1.1.7, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the CFG[CDIR] parameter.	2008-10-20	9.3	CVE-2008-4624 XF BID MILW0RM FRSIRT SECUNIA
gnu -- enscript	Stack-based buffer overflow in the read_special_escape function in src/psgen.c in GNU Enscript 1.6.1 and 1.6.4 beta, when the -e (aka special escapes processing) option is enabled, allows user-assisted remote attackers to execute arbitrary code via a crafted ASCII file, related to the setfilename command.	2008-10-23	7.6	CVE-2008-3863 XF BID BUGTRAQ MISC SECUNIA
goodtechsystems -- goodtech_ssh	Stack-based buffer overflow in the SFTP subsystem in GoodTech SSH 6.4 allows remote authenticated users to execute arbitrary code via a long string to the (1) open (aka SSH_FXP_OPEN), (2) unlink, (3) opendir, and other unspecified parameters.	2008-10-23	9.0	CVE-2008-4726 BID MILW0RM FRSIRT SECUNIA
hummingbird -- deployment_wizard	Multiple insecure method vulnerabilities in the DeployRun.DeploymentSetup.1 (DeployRun.dll) ActiveX control 10.0.0.44 in Hummingbird Deployment Wizard 2008 allow remote attackers to execute arbitrary programs via the (1) Run and (2) PerformUpdateAsync methods, and (3) modify arbitrary registry values via the SetRegistryValueAsString method. NOTE: the SetRegistryValueAsString method could be leveraged for code execution by specifying executable file values to Startup folders.	2008-10-23	9.3	CVE-2008-4728 MISC MISC MISC MILW0RM MILW0RM MILW0RM FRSIRT SECUNIA
ibm -- websphere_application_server	The HTTP_Request_Parser method in the HTTP Transport component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.31 allows remote attackers to cause a denial of service (controller 0C4 abend and application hang) via a long HTTP Host header, related to "storage overlay" on the stack and a "parse failure."	2008-10-22	7.8	CVE-2008-4678 XF BID FRSIRT AIXAPAR CONFIRM SECUNIA
ibm -- db2	The Native Managed Provider for .NET component in IBM DB2 8 before FP17, 9.1 before FP6, and 9.5 before FP2, when a definer cannot maintain objects, preserves views and triggers without marking them inoperative or dropping them, which has unknown impact and attack vectors.	2008-10-22	10.0	CVE-2008-4692 CONFIRM SECUNIA CONFIRM
joomla -- com_ds-syndicate	SQL injection vulnerability in the DS-Syndicate (com_ds-syndicate) component 1.1.1 for Joomla allows remote attackers to execute arbitrary SQL commands via the feed_id parameter to index2.php.	2008-10-20	7.5	CVE-2008-4623 XF BID MILW0RM FRSIRT SECUNIA

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
joomla -- com_imagebrowser	Directory traversal vulnerability in the Image Browser (com_imagebrowser) 0.1.5 component for Joomla! allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the folder parameter to index.php.	2008-10-22	9.0	CVE-2008-4668 XF BID MILW0RM
joomla -- joomla	SQL injection vulnerability in the Jpad (com_jpad) 1.0 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the cid parameter to index.php.	2008-10-23	7.5	CVE-2008-4715 XF BID MILW0RM
libspf -- libspf2	Heap-based buffer overflow in the SPF_dns_resolv_lookup function in Spf_dns_resolv.c in libspf2 before 1.2.8 allows remote attackers to execute arbitrary code via a long DNS TXT record with a modified length field.	2008-10-23	10.0	CVE-2008-2469 CERT-VN
linux -- kernel	The Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.27 does not properly handle a protocol violation in which a parameter has an invalid length, which allows attackers to cause a denial of service (panic) via unspecified vectors, related to sctp_sf_violation_paramlen, sctp_sf_abort_violation, sctp_make_abort_violation, and incorrect data types in function calls.	2008-10-20	7.8	CVE-2008-4618 MLIST CONFIRM CONFIRM
lynx -- lynx	lynx 2.8.6dev.15 and earlier, when advanced mode is enabled and lynx is configured as a URL handler, allows remote attackers to execute arbitrary commands via a crafted lynxcgi: URL, a related issue to CVE-2005-2929. NOTE: this might only be a vulnerability in limited deployments that have defined a lynxcgi: handler.	2008-10-22	10.0	CVE-2008-4690 MLIST
mantis -- mantis	manage_proj_page.php in Mantis before 1.1.4 allows remote authenticated users to execute arbitrary code via a sort parameter containing PHP sequences, which are processed by create_function within the multi_sort function in core/utility_api.php.	2008-10-22	9.0	CVE-2008-4687 CONFIRM MLIST MILW0RM CONFIRM CONFIRM CONFIRM
mantis -- mantis	Mantis before 1.1.3 does not unset the session cookie during logout, which makes it easier for remote attackers to hijack sessions.	2008-10-22	7.5	CVE-2008-4689 MLIST CONFIRM CONFIRM CONFIRM
michael_christen -- yacy	Multiple unspecified vulnerabilities in YaCy before 0.61 have unknown impact and attack vectors.	2008-10-24	10.0	CVE-2008-4731 BID SECUNIA CONFIRM
microsoft -- peachtree_accounting	Insecure method vulnerability in the ActiveX control (PAWWeb11.ocx) in Peachtree Accounting 2004 allows remote attackers to	2008-10-22	9.3	CVE-2008-4699 XF SECTRACK

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	execute arbitrary programs via the ExecutePreferredApplication method.			BID MILW0RM MISC
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_vista microsoft -- windows_xp	The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request, as exploited in the wild in October 2008, aka "Server Service Vulnerability."	2008-10-23	10.0	CVE-2008-4250 CERT-VN
midgard -- midgard_components_framework	Multiple unspecified vulnerabilities in Midgard Components (MidCOM) Framework before 8.09.1 have unknown impact and attack vectors.	2008-10-20	10.0	CVE-2008-4630 SECUNIA CONFIRM
mitre -- sezhoo	PHP remote file inclusion vulnerability in SezHooTabsAndActions.php in SezHoo 0.1 allows remote attackers to execute arbitrary PHP code via a URL in the IP parameter.	2008-10-23	7.5	CVE-2008-4704 BID MILW0RM
mosaic_commerce -- mosaic_commerce	SQL injection vulnerability in category.php in Mosaic Commerce allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2008-10-17	7.5	CVE-2008-4599 XF BID MILW0RM SECUNIA
mrbs -- mrbs	SQL injection vulnerability in Meeting Room Booking System (MRBS) before 1.4 allows remote attackers to execute arbitrary SQL commands via the area parameter to (1) month.php, and possibly (2) day.php and (3) week.php.	2008-10-20	7.5	CVE-2008-4620 XF BID MILW0RM FRSIRT
myer_sound_laboratories -- muscle	Stack-based buffer overflow in the Message::AddToString function in message/Message.cpp in MUSCLE before 4.40 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted message. NOTE: some of these details are obtained from third party information.	2008-10-20	10.0	CVE-2008-4631 CONFIRM XF SECUNIA
mywebland -- minibloggie	SQL injection vulnerability in del.php in myWebland miniBloggie 1.0 allows remote attackers to execute arbitrary SQL commands via the post_id parameter.	2008-10-20	7.5	CVE-2008-4628 XF BID MILW0RM FRSIRT
mywebland -- mystats	SQL injection vulnerability in hits.php in myWebland myStats allows remote attackers to execute arbitrary SQL commands via the sortby parameter.	2008-10-21	7.5	CVE-2008-4643 BID MILW0RM SECUNIA
mywebland -- mystats	hits.php in myWebland myStats allows remote attackers to bypass IP address restrictions via a modified X-Forwarded-For HTTP header.	2008-10-21	7.5	CVE-2008-4644 BID MILW0RM SECUNIA

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
mywebland -- myevent	SQL injection vulnerability in viewevent.php in myEvent 1.6 allows remote attackers to execute arbitrary SQL commands via the eventdate parameter.	2008-10-21	7.5	CVE-2008-4650 BID MILW0RM
openengine -- openengine	PHP remote file inclusion vulnerability in cms/classes/openengine/filepool.php in openEngine 2.0 beta2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the oe_classpath parameter, a different vector than CVE-2008-4329.	2008-10-23	9.3	CVE-2008-4719 BID MILW0RM
opera -- opera opera -- opera9.50 opera_software -- opera	Unspecified vulnerability in Opera before 9.60 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a redirect that specifies a crafted URL.	2008-10-23	9.3	CVE-2008-4694 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM MLIST MLIST FRSIRT SECTRACK
opera -- opera	Opera before 9.60 allows remote attackers to obtain sensitive information and have unspecified other impact by predicting the cache pathname of a cached Java applet and then launching this applet from the cache, leading to applet execution within the local-machine context.	2008-10-23	9.3	CVE-2008-4695 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM MLIST MLIST FRSIRT SECTRACK
php_jabbers -- post_comment	PHP Jabbers Post Comment 3.0 allows remote attackers to bypass authentication and gain administrative access by setting the PostCommentsAdmin cookie to "logged."	2008-10-23	7.5	CVE-2008-4721 MILW0RM
phpcounter -- phpcounter	SQL injection vulnerability in index.php in PHPcounter 1.3.2 and earlier allows remote attackers to execute arbitrary SQL commands via the name parameter.	2008-10-22	7.5	CVE-2008-4675 XF BID MILW0RM
phpfastnews -- phpfastnews	The isLoggedIn function in fastnews-code.php in phpFastNews 1.0.0 allows remote attackers to bypass authentication and gain administrative access by setting the fn-loggedin cookie to 1.	2008-10-20	7.5	CVE-2008-4622 XF BID MILW0RM FRSIRT SECUNIA
phponlinedatingsoftware -- myphpdating	SQL injection vulnerability in success_story.php in php Online Dating Software MyPHPDating allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-23	7.5	CVE-2008-4705 BID MILW0RM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
phpwebgallery -- phpwebgallery	plugins/event_tracer/event_list.php in PhpWebGallery 1.7.2 and earlier allows remote authenticated administrators to execute arbitrary PHP code via PHP sequences in the sort parameter, which is processed by create_function.	2008-10-21	9.0	CVE-2008-4645 BID
phpwebgallery -- phpwebgallery	Multiple directory traversal vulnerabilities in PhpWebGallery 1.3.4 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) user[language] and (2) user[template] parameters to (a) init.inc.php, and (b) the user[language] parameter to isadmin.inc.php.	2008-10-22	7.5	CVE-2008-4702 MILW0RM
pilot_group -- etraining	SQL injection vulnerability in news_read.php in Pilot Group (PG) eTraining allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-23	7.5	CVE-2008-4709 BID MILW0RM SECUNIA
pressography -- wp_comment_remix_plugin	SQL injection vulnerability in ajax_comments.php in the WP Comment Remix plugin before 1.4.4 for WordPress allows remote attackers to execute arbitrary SQL commands via the p parameter.	2008-10-24	7.5	CVE-2008-4732 BID
pressography -- wp_comment_remix_plugin	Cross-site request forgery (CSRF) vulnerability in the wpcr_do_options_page function in WP Comment Remix plugin before 1.4.4 for WordPress allows remote attackers to perform unauthorized actions as administrators via a request that sets the wpcr_hidden_form_input parameter.	2008-10-24	7.5	CVE-2008-4734 XF BUGTRAQ SECUNIA MISC
pyxicom -- actualite	SQL injection vulnerability in the actualite module 1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-20	7.5	CVE-2008-4617 XF BID MILW0RM
qvod -- qvod_player	Heap-based buffer overflow in QvodInsert.QvodCtrl.1 ActiveX control (QvodInsert.dll) in QVOD Player before 2.1.5 build 0053 allows remote attackers to execute arbitrary code via a long URL property. NOTE: some of these details are obtained from third party information.	2008-10-21	9.3	CVE-2008-4664 BID SECUNIA
rgallery -- rgallery_plugin	SQL injection vulnerability in the rGallery plugin 1.09 for WoltLab Burning Board (WBB) allows remote attackers to execute arbitrary SQL commands via the itemID parameter in the RGalleryImageWrapper page in index.php.	2008-10-20	7.5	CVE-2008-4627 BID MILW0RM SECUNIA
scriptdemo -- php-lance	SQL injection vulnerability in show.php in BitmixSoft PHP-Lance 1.52 allows remote attackers to execute arbitrary SQL commands via the catid parameter.	2008-10-23	7.5	CVE-2008-4716 BID MILW0RM SECUNIA

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
sentex -- jhead	The DoCommand function in jhead.c in Matthias Wandel jhead 2.84 and earlier allows attackers to execute arbitrary commands via shell metacharacters in unspecified input.	2008-10-21	10.0	CVE-2008-4641 CONFIRM MLIST MLIST MLIST
shiftthis -- shifthis_newsletter	SQL injection vulnerability in stnl_iframe.php in the ShiftThis Newsletter (st_newsletter) plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the newsletter parameter, a different vector than CVE-2008-0683.	2008-10-20	7.5	CVE-2008-4625 XF BID MILW0RM
slaytanic_scripts -- content_plus	Multiple unspecified vulnerabilities in Slaytanic Scripts Content Plus 2.1.1 have unknown impact and remote attack vectors.	2008-10-17	10.0	CVE-2008-4595 XF BID CONFIRM SECUNIA
sun -- solaris	The RPC subsystem in Sun Solaris 9 allows remote attackers to cause a denial of service (daemon crash) via a crafted request to procedure 8, related to the XDR_DECODE operation and the taddr2uaddr function.	2008-10-20	10.0	CVE-2008-4619 MILW0RM
sun -- integrated_lights-out_manager sun -- blade_6000_modular_system_with_chassis sun -- blade_6048_modular_system_with_chassis sun -- blade_8000_modular_system sun -- blade_8000p_modular_system sun -- blade_t6320_server_module sun -- blade_x6220_with_server_module_software sun -- blade_x6250_with_server_module_software sun -- blade_x6450_with_server_module_software sun -- blade_x8400 sun -- blade_x8420 sun -- blade_x8440 sun -- blade_x8450 sun -- fire_x2250_server sun -- fire_x4100_server sun -- fire_x4100m2_server sun -- fire_x4140_server sun -- fire_x4150_server sun -- fire_x4200_server sun -- fire_x4200m2_server sun -- fire_x4240_server sun -- fire_x4250_server sun -- fire_x4440_server sun -- fire_x4450_server sun -- fire_x4500_server sun -- fire_x4540_server sun -- fire_x4600_server sun -- fire_x4600m2_server	Unspecified vulnerability in Sun Integrated Lights-Out Manager (ILOM) 2.0.1.5 through 2.0.4.26 allows remote authenticated users to (1) access the service processor (SP) and cause a denial of service (shutdown or reboot), or (2) access the host operating system and have an unspecified impact, via unknown vectors.	2008-10-23	9.0	CVE-2008-4722 FRSIRT

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
sun -- netra sun -- netra_x4200m2_server sun -- netra_x4250_server sun -- netra_x4450 sun -- sparc_enterprise_server_t5120 sun -- sparc_enterprise_server_t5140 sun -- sparc_enterprise_server_t5220 sun -- sparc_enterprise_server_t5240 sun -- sparc_enterprise_server_t5440				
sweetcms -- sweetcms	SQL injection vulnerability in index.php in sweetCMS 1.5.2 allows remote attackers to execute arbitrary SQL commands via the page parameter.	2008-10-21	7.5	CVE-2008-4647 SECUNIA MISC
sylvain_pasquet -- bbzl.php	BbZL.PhP 0.92 allows remote attackers to bypass authentication and gain administrative access by setting the phorum_admin_session cookie to 1.	2008-10-23	7.5	CVE-2008-4708 BID MILW0RM
trend_micro -- officescan	Stack-based buffer overflow in CGI programs in the server in Trend Micro OfficeScan 7.3 Patch 4 build 1367 and other builds before 1374, and 8.0 SP1 Patch 1 before build 3110, allows remote attackers to execute arbitrary code via an HTTP POST request containing crafted form data, related to "parsing CGI requests."	2008-10-23	10.0	CVE-2008-3862 CONFIRM CONFIRM SECUNIA
tufat -- mycard	SQL injection vulnerability in gallery.php in MyCard 1.0.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-24	7.5	CVE-2008-4738 BID MILW0RM SECUNIA
typo3 -- simplesurvey	SQL injection vulnerability in the Simple survey (simplesurvey) 1.7.0 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-10-21	7.5	CVE-2008-4655 CONFIRM CONFIRM
typo3 -- frontend_users_view	SQL injection vulnerability in the Frontend Users View (feusersview) 0.1.6 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-10-21	7.5	CVE-2008-4656 BID CONFIRM
typo3 -- econda_plugin	SQL injection vulnerability in the Econda Plugin (econda) 0.0.2 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-10-21	7.5	CVE-2008-4657 BID CONFIRM
typo3 -- jobcontrol	SQL injection vulnerability in the JobControl (dmmjobcontrol) 1.15.4 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-10-21	7.5	CVE-2008-4658 BID CONFIRM MISC
typo3 -- mannschaftsliste	SQL injection vulnerability in the Mannschaftsliste (kiddog_playerlist) 1.0.3 and earlier extension for TYPO3 allows remote	2008-10-21	7.5	CVE-2008-4659 BID CONFIRM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	attackers to execute arbitrary SQL commands via unspecified vectors.			
typo3 -- m1_intern	SQL injection vulnerability in the M1 Intern (m1_intern) 1.0.0 extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-10-21	7.5	CVE-2008-4660 BID CONFIRM
vbulletin -- vbgooglemap	SQL injection vulnerability in VBGooglemap Hotspot Edition 1.0.3, a vBulletin module, allows remote attackers to execute arbitrary SQL commands via the mapid parameter in a showdetails action to (1) vbgooglemaphse.php and (2) mapa.php.	2008-10-23	7.5	CVE-2008-4706 BID MILW0RM SECUNIA
videolan -- vlc_media_player	Stack-based buffer overflow in the parse_master function in the Ty demux plugin (modules/demux/ty.c) in VLC Media Player 0.9.0 through 0.9.4 allows remote attackers to execute arbitrary code via a TiVo TY media file with a header containing a crafted size value.	2008-10-21	9.3	CVE-2008-4654 XF CONFIRM MISC BID BUGTRAQ MLIST FRSIRT SECUNIA CONFIRM CONFIRM CONFIRM
videolan -- vlc_media_player	Multiple integer overflows in ty.c in the TY demux plugin (aka the TiVo demuxer) in VideoLAN VLC media player, probably 0.9.4, allow remote attackers to have an unknown impact via a crafted .ty file, a different vulnerability than CVE-2008-4654.	2008-10-22	9.3	CVE-2008-4686 MLIST CONFIRM
webbiscuits -- events_calendar	PHP remote file inclusion vulnerability in panel/common/theme/default/header_setup.php in WebBiscuits Software Events Calendar 1.1 allows remote attackers to execute arbitrary PHP code via a URL in the (1) path[docroot] and (2) component parameters.	2008-10-22	10.0	CVE-2008-4673 XF BID MILW0RM FRSIRT SECUNIA
x7_group -- x7_chat	Directory traversal vulnerability in help/mini.phpin X7 Chat 2.0.1 A1 and earlier allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the help_file parameter, a different vector than CVE-2006-2156.	2008-10-23	7.5	CVE-2008-4718 MILW0RM MILW0RM
xoops -- makale	SQL injection vulnerability in makale.php in Makale 0.26 and possibly other versions, a module for XOOPS, allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: some of these details are obtained from third party information.	2008-10-21	7.5	CVE-2008-4653 BID MILW0RM SECUNIA
zeescripts -- zeeproperty	SQL injection vulnerability in bannerclick.php in ZeeScripts Zeeproperty allows remote attackers to execute arbitrary SQL commands via the adid parameter.	2008-10-20	7.5	CVE-2008-4621 XF BID MILW0RM FRSIRT

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
				SECUNIA
zeeways -- zeelyrics	SQL injection vulnerability in bannerclick.php in ZEELYRICS 2.0 allows remote attackers to execute arbitrary SQL commands via the adid parameter.	2008-10-23	7.5	CVE-2008-4717 BID MILW0RM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
cisco -- asa_5500 cisco -- pix	Unspecified vulnerability in Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.0 before 7.0(8)3, 7.1 before 7.1(2)78, 7.2 before 7.2(4)16, 8.0 before 8.0(4)6, and 8.1 before 8.1(1)13, when configured as a VPN using Microsoft Windows NT Domain authentication, allows remote attackers to bypass VPN authentication via unknown vectors.	2008-10-23	4.3	CVE-2008-3815 XF BID CISCO
citrix -- access_essentials citrix -- presentation_server citrix -- xenapp	Unspecified vulnerability in Citrix XenApp (formerly Presentation Server) 4.5 Feature Pack 1 and earlier, Presentation Server 4.0, and Access Essentials 1.0, 1.5, and 2.0 allows local users to gain privileges via unknown attack vectors related to creating an unspecified file. NOTE: this might be the same issue as CVE-2008-3485, but the vendor advisory is too vague to be certain.	2008-10-22	6.8	CVE-2008-4676 CONFIRM
conkurent -- real_estate	SQL injection vulnerability in realestate-index.php in Conkurent Real Estate Manager 1.01 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in browse mode.	2008-10-22	6.8	CVE-2008-4674 XF BID MILW0RM SECUNIA
cpcommerce -- cpcommerce	Multiple cross-site scripting (XSS) vulnerabilities in cpCommerce before 1.2.4 allow remote attackers to inject arbitrary web script or HTML via (1) the search parameter in a search.quick action to search.php and (2) the name parameter in a sendtofriend action to sendtofriend.php.	2008-10-21	4.3	CVE-2008-4121 BUGTRAQ MISC SECUNIA CONFIRM
cpcommerce -- cpcommerce	Cross-site scripting (XSS) vulnerability in cpCommerce before 1.2.4 allows remote attackers to inject arbitrary web script or HTML via unknown vectors in the advanced search feature. NOTE: this is probably a variant of CVE-2008-4121.	2008-10-21	4.3	CVE-2008-4637 CONFIRM
dan_fletcher -- recipe_script	Cross-site scripting (XSS) vulnerability in search.php in Dan Fletcher Recipe Script allows remote attackers to inject arbitrary web script or HTML via the keyword parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-22	4.3	CVE-2008-4669 XF MISC BID
deeserver -- ultimate_webboard	SQL injection vulnerability in webboard.php in Ultimate Webboard 3.00 allows remote attackers to execute arbitrary SQL commands via the Category parameter.	2008-10-22	6.8	CVE-2008-4666 XF BID MILW0RM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
drupal -- node_clone	SQL injection vulnerability in Node Vote 5.x before 5.x-1.1 and 6.x before 6.x-1.0, a module for Drupal, when "Allow user to vote again" is enabled, allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors related to a "previously cast vote."	2008-10-20	6.0	CVE-2008-4633 XF BID SECUNIA CONFIRM
drupal -- stock_module	Cross-site scripting (XSS) vulnerability in the stock quotes page in Stock 6.x before 6.x-1.0, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-10-23	4.3	CVE-2008-4710 XF BID CONFIRM
ed_putal -- clickbank_portal	Cross-site scripting (XSS) vulnerability in search.php in Ed Pudol Clickbank Portal allows remote attackers to inject arbitrary web script or HTML via the search box. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-22	4.3	CVE-2008-4670 XF MISC BID
elxis -- elxis_cms	Cross-site scripting (XSS) vulnerability in index.php in Elxis CMS 2008.1 revision 2204 allows remote attackers to inject arbitrary web script or HTML via the (1) PATH_INFO or the (2) option, (3) Itemid, (4) id, (5) task, (6) bid, and (7) contact_id parameters. NOTE: the error might be located in modules/mod_language.php, and index.php might be the interaction point.	2008-10-21	4.3	CVE-2008-4648 XF BID SECUNIA MISC
goodlyrics -- lyrics_script	Cross-site scripting (XSS) vulnerability in search_results.php in buymyscripts Lyrics Script allows remote attackers to inject arbitrary web script or HTML via the k parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-22	4.3	CVE-2008-4672 XF MISC BID
google -- chrome	Multiple cross-site scripting (XSS) vulnerabilities in Google Chrome 0.2.149.30 allow remote attackers to inject arbitrary web script or HTML via an ftp:// URL for an HTML document within a (1) JPG, (2) PDF, or (3) TXT file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-23	4.3	CVE-2008-4724 BID
habari -- cms	Cross-site scripting (XSS) vulnerability in the login feature in Habari CMS 0.5.1 allows remote attackers to inject arbitrary web script or HTML via the habari_username parameter.	2008-10-17	4.3	CVE-2008-4601 XF BID SECUNIA MISC
hisanaga_electric_co -- hisa_cart	Unspecified vulnerability in Hisanaga Electric Co, Ltd. hisa_cart 1.29 and earlier, a module for XOOPS, allows remote attackers to obtain sensitive user information via unknown vectors.	2008-10-20	5.0	CVE-2008-4635 XF BID SECUNIA JVNDB JVN CONFIRM
hp -- systems_insight_manager	Unspecified vulnerability in HP Systems Insight Manager (SIM) before 5.2 Update 2 (C.05.02.02.00) allows remote attackers to obtain sensitive information via unspecified vectors.	2008-10-17	5.0	CVE-2008-4412 HP

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
hp -- sitescope	Cross-site scripting (XSS) vulnerability in the management interface in HP SiteScope 9.0 build 911 allows remote attackers to inject arbitrary web script or HTML via an SNMP trap message.	2008-10-21	4.3	CVE-2007-4350 XF BID BUGTRAQ FRSIRT SECTRACK MISC SECUNIA
hp -- openview_report hp -- performance_agent	The Shared Trace Service (aka OVTrace) in HP OpenView Report 3.70 and Performance Agent 4.70 allows remote attackers to cause a denial of service via an unspecified series of RPC requests that triggers an out-of-bounds memory access, related to an erroneous object reference.	2008-10-23	4.3	CVE-2007-4349 XF BID BUGTRAQ FRSIRT MISC SECUNIA
hummingbird -- exceed hummingbird -- exceed_powersuite	Stack-based buffer overflow in Hummingbird.XWebHostCtrl.1 ActiveX control (hclxweb.dll) in Hummingbird Xweb ActiveX Control 13.0 and earlier allows remote attackers to execute arbitrary code via a long PlainTextPassword property. NOTE: code execution might not be possible in 13.0.	2008-10-23	6.8	CVE-2008-4729 MILW0RM SECUNIA
ibm -- websphere_application_server	The Web Services Security component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.31 and 6.1 before 6.1.0.19, when Certificate Store Collections is configured to use Certificate Revocation Lists (CRL), does not call the setRevocationEnabled method on the PKIXBuilderParameters object, which prevents the "Java security method" from checking the revocation status of X.509 certificates and allows remote attackers to bypass intended access restrictions via a SOAP message with a revoked certificate.	2008-10-22	6.8	CVE-2008-4679 AIXAPAR CONFIRM CONFIRM
ibm -- db2	Unspecified vulnerability in the SQLNLS_UNPADDEDCHARLEN function in the New Compiler (aka Starburst derived compiler) component in the server in IBM DB2 9.1 before FP6 allows attackers to cause a denial of service (segmentation violation and trap) via unknown vectors.	2008-10-22	5.0	CVE-2008-4691 CONFIRM AIXAPAR SECUNIA CONFIRM
ibm -- db2	The SORT/LIST SERVICES component in IBM DB2 9.1 before FP6 and 9.5 before FP2 writes sensitive information to the trace output, which allows attackers to obtain sensitive information by reading "PASSWORD-RELATED CONNECTION STRING KEYWORD VALUES."	2008-10-22	5.0	CVE-2008-4693 CONFIRM SECUNIA CONFIRM
jetbox -- jetbox_cms	Multiple SQL injection vulnerabilities in Jetbox CMS 2.1 allow remote authenticated users to execute arbitrary SQL commands via the (1) orderby parameter to admin/cms/images.php and the (2) nav_id parameter in an editrecord action to admin/cms/nav.php.	2008-10-21	6.0	CVE-2008-4651 XF BID MISC
joovili -- joovili	SQL injection vulnerability in Joovili 3.0 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the id parameter to (1) view.blog.php, (2) view.event.php, (3) view.group.php, (4) view.music.php, (5) view.picture.php, and (6)	2008-10-23	6.8	CVE-2008-4711 BID MILW0RM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	view.video.php.			
kumacchi -- ks_cgi_access_log	Cross-site scripting (XSS) vulnerability in analysis.cgi 1.44, as used in K's CGI Access Log Kaiseki (1) jcode.pl and (2) Jcode.pm, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-10-21	4.3	CVE-2008-4663 CONFIRM CONFIRM JVNDB JVNDB JVN JVN
kure -- kure	Multiple directory traversal vulnerabilities in index.php in Kure 0.6.3, when magic_quotes_gpc is disabled, allow remote attackers to read and possibly execute arbitrary local files via a .. (dot dot) in the (1) post and (2) doc parameters.	2008-10-20	6.8	CVE-2008-4632 XF BID MILW0RM
liberiacms -- liberia_cms	SQL injection vulnerability in admin.php in Libera CMS 1.12 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the libera_staff_pass cookie parameter.	2008-10-22	6.8	CVE-2008-4700 XF BID MILW0RM SECUNIA
liberiacms -- liberia_cms	SQL injection vulnerability in admin.php in Libera CMS 1.12, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the libera_staff_user cookie parameter, a different vector than CVE-2008-4700. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-22	6.8	CVE-2008-4701 XF SECUNIA
lnblog -- lnblog	Directory traversal vulnerability in pages/showblog.php in LnBlog 0.9.0 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the plugin parameter.	2008-10-23	6.8	CVE-2008-4712 BID MILW0RM SECUNIA
lokicms -- lokicms	Directory traversal vulnerability in admin.php in LokiCMS 0.3.4, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the language parameter.	2008-10-21	6.8	CVE-2008-4662 BID
mantis -- mantis	core/string_api.php in Mantis before 1.1.3 does not check the privileges of the viewer before composing a link with issue data in the source anchor, which allows remote attackers to discover an issue's title and status via a request with a modified issue number.	2008-10-22	5.0	CVE-2008-4688 MLIST CONFIRM CONFIRM CONFIRM
microsoft -- exchange_server	Open redirect vulnerability in exchweb/bin/redir.asp in Microsoft Outlook Web Access (OWA) for Exchange Server 2003 SP2 (aka build 6.5.7638) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the URL parameter.	2008-10-20	4.3	CVE-2008-1547 BID BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ
mozilla -- firefox	Multiple cross-site scripting (XSS) vulnerabilities in Mozilla Firefox 3.0.1 through 3.0.3 allow remote attackers to inject arbitrary web script or HTML via an ftp:// URL for an HTML document within a (1) JPG, (2) PDF, or (3) TXT file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party	2008-10-23	4.3	CVE-2008-4723 BID

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	information.			
noc2 -- whodomlite	Cross-site scripting (XSS) vulnerability in wholite.cgi in WhoDomLite 1.1.3 allows remote attackers to inject arbitrary web script or HTML via the dom parameter.	2008-10-24	4.3	CVE-2008-4737 MISC BID OSVDB SECUNIA
opera -- opera	Cross-site scripting (XSS) vulnerability in Opera.dll in Opera before 9.61 allows remote attackers to inject arbitrary web script or HTML via the anchor identifier (aka the "optional fragment"), which is not properly escaped before storage in the History Search database (aka md.dat).	2008-10-23	4.3	CVE-2008-4696 BID CONFIRM CONFIRM CONFIRM
opera -- opera opera -- opera9.50 opera_software -- opera	The Fast Forward feature in Opera before 9.61, when a page is located in a frame, executes a javascript: URL in the context of the outermost page instead of the page that contains this URL, which allows remote attackers to conduct cross-site scripting (XSS) attacks.	2008-10-23	4.3	CVE-2008-4697 XF BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM MLIST MLIST FRSIRT SECUNIA
opera -- opera opera -- opera9.50 opera_software -- opera	Opera before 9.61 does not properly block scripts during preview of a news feed, which allows remote attackers to create arbitrary new feed subscriptions and read the contents of arbitrary feeds.	2008-10-23	5.8	CVE-2008-4698 XF BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM MLIST MLIST FRSIRT SECUNIA
opera -- opera opera -- opera9.50 opera_software -- opera	Cross-site scripting (XSS) vulnerability in Opera.dll in Opera 9.52 allows remote attackers to inject arbitrary web script or HTML via the query string, which is not properly escaped before storage in the History Search database (aka md.dat), a different vector than CVE-2008-4696. NOTE: some of these issues were addressed before 9.60.	2008-10-23	4.3	CVE-2008-4725 XF BID BUGTRAQ MISC MISC MISC MISC MISC MISC MISC MLIST MLIST MILW0RM FRSIRT SECUNIA

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
phpmyid -- phpmyid	Cross-site scripting (XSS) vulnerability in MyID.php in phpMyID 0.9 allows remote attackers to inject arbitrary web script or HTML via the openid_trust_root parameter and an inconsistent openid_return_to parameter, which is not properly handled in an error message.	2008-10-24	4.3	CVE-2008-4730 BUGTRAQ
plugspace -- plugspace	Directory traversal vulnerability in index.php in PlugSpace 0.1, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the navi parameter.	2008-10-24	6.8	CVE-2008-4739 BID MILW0RM SECUNIA
pressography -- wp_comment_remix_plugin	Cross-site scripting (XSS) vulnerability in wpcommentremix.php in WP Comment Remix plugin before 1.4.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the (1) replytotext, (2) quotetext, (3) originallypostedby, (4) sep, (5) maxtags, (6) tagsep, (7) tagheadersep, (8) taglabel, and (9) tagheaderlabel parameters.	2008-10-24	4.3	CVE-2008-4733 XF BID BUGTRAQ SECUNIA MISC
sentex -- jhead	jhead.c in Matthias Wandel jhead before 2.84 allows local users to overwrite arbitrary files via a symlink attack on a temporary file.	2008-10-21	4.6	CVE-2008-4639 CONFIRM MLIST MLIST MLIST
sungard -- banner_student	Cross-site scripting (XSS) vulnerability in the contact update page (ss/bwgkoemr.P_UpdateEmrgContacts) in SunGard Banner Student 7.3 allows remote attackers to inject arbitrary web script or HTML via the addr1 parameter. NOTE: this might be resultant from a CSRF vulnerability, but there are insufficient details to be sure.	2008-10-23	4.3	CVE-2008-4727 BID BUGTRAQ MISC
sylvain_pasquet -- bbzl_php	Directory traversal vulnerability in index.php in BbZL.PhP 0.92 allows remote attackers to access unauthorized directories via a .. (dot dot) in the lien_2 parameter.	2008-10-23	5.0	CVE-2008-4707 BID MILW0RM
symantec -- veritas_file_system	qiomkfile in the Quick I/O for Database feature in Symantec Veritas File System (VxFS) on HP-UX, and before 5.0 MP3 on Solaris, Linux, and AIX, does not initialize filesystem blocks during creation of a file, which allows local users to obtain sensitive information by creating and then reading files.	2008-10-21	4.6	CVE-2008-3248 CONFIRM CONFIRM
symantec -- veritas_file_system	qioadmin in the Quick I/O for Database feature in Symantec Veritas File System (VxFS) on HP-UX, and before 5.0 MP3 on Solaris, Linux, and AIX, allows local users to read arbitrary files by causing qioadmin to write a file's content to standard error.	2008-10-21	4.6	CVE-2008-4638 CONFIRM CONFIRM
typo3 -- page_improvements	Cross-site scripting (XSS) vulnerability in the Page Improvements (sm_pageimprovements) 1.1.0 and earlier extension for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-10-21	4.3	CVE-2008-4661 CONFIRM MISC
usagi -- mynets	Cross-site scripting (XSS) vulnerability in Usagi Project MyNETS 1.2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-10-20	4.3	CVE-2008-4629 CONFIRM SECUNIA JVNDB JVN

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
vim -- netrw	autoload/netrw.vim (aka the Netrw Plugin) 109, 131, and other versions before 133k for Vim 7.1.266, other 7.1 versions, and 7.2 stores credentials for an FTP session, and sends those credentials when attempting to establish subsequent FTP sessions to servers on different hosts, which allows remote FTP servers to obtain sensitive information in opportunistic circumstances by logging usernames and passwords. NOTE: the upstream vendor disputes a vector involving different ports on the same host, stating "I'm assuming that they're using the same id and password on that unchanged hostname, deliberately."	2008-10-22	4.3	CVE-2008-4677 CONFIRM MISC MLIST MLIST MLIST SECUNIA MLIST
wireshark -- wireshark	packet-usb.c in the USB dissector in Wireshark 0.99.7 through 1.0.3 allows remote attackers to cause a denial of service (application crash or abort) via a malformed USB Request Block (URB).	2008-10-22	4.3	CVE-2008-4680 BID
wireshark -- wireshark	Unspecified vulnerability in the Bluetooth RFCOMM dissector in Wireshark 0.99.7 through 1.0.3 allows remote attackers to cause a denial of service (application crash or abort) via unknown packets.	2008-10-22	4.3	CVE-2008-4681 BID
wireshark -- wireshark	wtap.c in Wireshark 0.99.7 through 1.0.3 allows remote attackers to cause a denial of service (application abort) via a malformed Tamos CommView capture file (aka .ncf file) with an "unknown/unexpected packet type" that triggers a failed assertion.	2008-10-22	5.0	CVE-2008-4682 BID
wireshark -- wireshark	The dissect_btacl function in packet-bthci_acl.c in the Bluetooth ACL dissector in Wireshark 0.99.2 through 1.0.3 allows remote attackers to cause a denial of service (application crash or abort) via a packet with an invalid length, related to an erroneous tvb_memcpy call.	2008-10-22	5.0	CVE-2008-4683 BID
wireshark -- wireshark	packet-frame in Wireshark 0.99.2 through 1.0.3 does not properly handle exceptions thrown by post dissectors, which allows remote attackers to cause a denial of service (application crash) via a certain series of packets, as demonstrated by enabling the (1) PRP or (2) MATE post dissector.	2008-10-22	4.3	CVE-2008-4684 BID FRSIRT
wireshark -- wireshark	Use-after-free vulnerability in the dissect_q931_cause_ie function in packet-q931.c in the Q.931 dissector in Wireshark 0.10.3 through 1.0.3 allows remote attackers to cause a denial of service (application crash or abort) via certain packets that trigger an exception.	2008-10-22	5.0	CVE-2008-4685 BID FRSIRT SECUNIA
wordpress -- wordpress_mu	Cross-site scripting (XSS) vulnerability in wp-admin/wp-blogs.php in Wordpress MU (WPMU) before 2.6 allows remote attackers to inject arbitrary web script or HTML via the (1) s and (2) ip_address parameters.	2008-10-22	4.3	CVE-2008-4671 BID SECUNIA FULLDISC
zirkon_box -- yappa-ng	Directory traversal vulnerability in index.php in Fritz Berger yet another php photo album - next generation (yappa-ng) 2.3.2 and possibly other versions through 2.3.3-beta0, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the album parameter.	2008-10-20	6.8	CVE-2008-4626 MILW0RM SECUNIA

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
sentex -- jhead	The DoCommand function in jhead.c in Matthias Wandel jhead 2.84 and earlier allows local users to delete arbitrary files via vectors involving a modified input filename in which (1) a final "z" character is replaced by a "t" character or (2) a final "t" character is replaced by a "z" character.	2008-10-21	3.6	CVE-2008-4640 CONFIRM MLIST
six_apart -- movable_type	Cross-site scripting (XSS) vulnerability in Movable Type 4 through 4.21 allows remote attackers to inject arbitrary web script or HTML via unknown vectors related to the administrative page, a different vulnerability than CVE-2008-4079.	2008-10-20	3.5	CVE-2008-4634 XF CONFIRM BID SECUNIA JVNDB JVN
websense -- enterpise	The Websense Reporter Module in Websense Enterprise 6.3.2 stores the SQL database system administrator password in plaintext in CreateDbInstall.log, which allows local users to gain privileges to the database.	2008-10-21	2.1	CVE-2008-4646 MISC SECTRACK BID FRSIRT SECUNIA

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
Back to top				